Statement of Steve DelBianco

Vice President for Public Policy,

The Association for Competitive Technology (ACT)

Testimony before the

House Committee on Small Business,

Subcommittee on Finance and Tax

Hearing on

"*Data Security: Small Business Perspectives*"

June 6, 2007

Chairwoman Bean, Ranking Member Heller, and distinguished members of the Committee: My name is Steve DelBianco, and I am Vice President for Public Policy for the Association for Competitive Technology (ACT). I would like to thank the Committee for holding this important hearing and I'm pleased to have the opportunity to testify on the impact of data security threats—and the threats of data security regulations—on small business.

ACT is an education and advocacy group for small, technology-based businesses. We represent over 3,000 small tech firms and e-commerce businesses, including many that accept credit card payments and handle sensitive customer data for testing or hosting customer billing and payroll applications.

ACT advocates for a "Healthy Tech Environment" that promotes innovation, competition and investment. Two indicators of a healthy tech environment are a high degree of consumer trust & confidence, and low regulatory burdens for businesses. Both these indicators are under attack from criminals who steal business information in order to pursue credit card fraud and identity theft.

I also come before you having made my own small business odyssey: In 1984 I founded an IT consulting firm, and grew it to $20 million in sales and 200 employees over 13 years, then sold the business to a national firm before helping to start ACT.

Data Protection is an important issue for small business, especially e-commerce retailers. Data protection legislation from the prior and current Congress would require consumer notification of a breach, and would require the implementation of security measures to safeguard consumer information. Notification and data security are distinct subjects and each matter could merit its own Congressional hearing. While several House bills combine the two issues, for purposes of this hearing and my testimony, it is helpful to separate notification from data protection when analyzing the regulatory impact on small businesses.

Why Data Security Regulation is So Expensive for Small Business

What's unique about the perspective of small business in assessing the impact of data protection regulation? The first two answers to this question are widely known:

- Fixed costs disproportionately impact small business, and this is equally true of costs for data protection measures required by regulation. The Securities Exchange Commission has reacted to widespread complaints that smaller businesses were chafing at the million-dollar cost of implementing financial reporting systems to comply with Sarbanes Oxley regulations.
- Small business is rarely at the table when laws and regulations are being crafted. This is not to suggest that lawmakers and agencies fail to consider the interests of small business. Indeed, the Regulatory Flexibility Act requires special analysis for proposed rules that "*would have a substantial economic impact on a substantial number of small entities*."[1] And when the FTC was preparing data safeguard rules pursuant to the Gramm-Leach-Bliley Act (GLB) back in 2002, it sought comments on the costs to small entities, but reported that "*no commenters provided specific cost information*."[2] Our government frequently asks for input, but it's not surprising that small business owners rarely scan the Federal Register or find the time to respond with specific cost information.

In addition, there are less obvious aspects to why small business is particularly vulnerable to new threats and new regulatory requirements:

- In a small business, the time and attention of top management is stretched thin. The top of the management pyramid in a small business is narrow (often just the owner), so their time is consumed by cash management and crisis management. To put it simply, a small business owner is usually too busy fighting fires to pay much mind to preventing new ones – even when they know they should.
- It's exceedingly rare for a small business to have in-house legal counsel or in-house expertise in the products and practices of information security. Nor do small businesses have a "bench" of talented executives to which they can delegate special projects, such as an initiative to improve data protection and regulatory compliance.

---

[1] Federal Register / Vol. 67, No. 100, May 23, 2002, Rules and Regulations by the Federal Trade Commission, regarding 16 CFR Part 314, "Standards for Safeguarding Customer Information; Final Rule", p. 36491.

[2] Ibid, p. 36491.

During the GLB rulemaking, a few trade associations told the FTC that small businesses would be disproportionately burdened "*because they lack expertise (relative to larger entities) in developing, implementing, and maintaining the required safeguards*"[3].

- Moreover, small businesses don't have the expertise to solicit, select, and manage outside vendors and consultants in areas that require specialization and experience. This "asymmetry of expertise" tends to make small business more susceptible to expensive implementation contracts and service agreements, especially when data security vendors are encouraged to mitigate risks by over-engineering their proposed solutions.

[3] Ibid, p. 36491.

THE CRIME AND COSTS OF IDENTITY THEFT

There are multiple victims in any consumer data breach. Consumers are the most obvious victims, but so too are the businesses that suffered the breach, particularly small business. When criminals breach customer data held by a small business, they place at risk the very survival of that company. It's essential to remember that although data can be lost many ways, "It takes a thief" to make data loss into a crime.

"It Takes a Thief" to Commit Identity Theft

With all of the press accounts, statistics, and assorted approaches to legislation, it seems we've lost sight of the root cause that's driving demand for data protection regulation. If a data tape falls off a delivery truck, or a sales rep loses her laptop computer, no crime has yet been committed. It takes a thief to turn these losses into crimes, by charging someone else's credit card or opening new credit accounts in their name.

Imagine a new series in the popular *CSI* genre: ***CSI: Identity Theft****:*

> The premier episode features a criminal gang called ShadowCrew, who's made a science out of identity fraud. They've got 4,000 gang members operating around the world using the latest technology to coordinate, communicate, and trade in stolen credit cards and identity documents.
>
> We meet the leader, a 20-something American business student who set-up a website to bring together buyers and sellers of stolen cards and data. We see several levels of ShadowCrew management, including "moderators" who host online forums to help members design convincing phishing emails, and to plant spyware on users' computers to steal passwords and account numbers.
>
> We meet the "reviewers," who rate the stolen information for quality and street value. There are "vendors" who package the goods for sale to gang members, often through online auctions. Everyone moves quickly and talks fast, since stolen cards have to be used before cardholders cancel their accounts.
>
> Then, cut to a nighttime scene in downtown Washington, where a team of Secret Service agents are using high-tech surveillance tools to monitor the gang, who's having an online group meeting. We hear the "Go!" order, and armed agents break-down doors to a dozen homes and apartments around the country. Some weapons are uncovered, and one gang member jumps from a second-story window, only to be apprehended by agents on the ground.

> As the credits roll, the narrator says, "*The events you have seen are true*..." The ShadowCrew bust really happened, on October 26, 2004[4].

This ShadowCrew episode reminds us that thieves are behind every fraudulent charge and credit account that's opened in someone else's name. And it demonstrates that identity thieves are professional, organized criminals, capable of large-scale operations: the Secret Service found 1.7 million credit card numbers, access keys for 18 million email accounts, and identity data for thousands of people in their ShadowCrew investigation.

ShadowCrew harvested much of their data by phishing, where consumers were duped into giving up their own information over the phone or online. But they also hacked into a dozen corporate systems, including banks and credit card networks.

Today, the ShadowCrew gang members are being prosecuted under the Computer Fraud & Abuse Act, which carries prison sentences up to 20 years. We need more high-profile prosecutions like this if we want to have any hope of deterring identity thieves and reducing the losses due to credit card fraud and identity theft.

Business Bears 90% of the Costs of Identity Theft

Obviously, card fraud artists and identity thieves are spending other people's money. In 2005, Tom Lenard and Paul Rubin of the Progress & Freedom Foundation helped us understand who is paying for 55 billion dollars in annual identity theft losses.[5] Nearly all of these losses happen through the misuse of credit accounts, which occurs in two ways:

> Two thirds of these incidents are someone running-up charges on a victim's credit card. In these incidents, the cardholder incurs an average of $160 in out-of-pocket costs, and spends about 15 hours refuting charges and canceling compromised accounts. The retail businesses who accepted the fraudulent charge incur another $2,100. The loss differential between the cardholder and businesses is no surprise, given that nearly all card issuers limit cardholders' exposure for fraudulent charges. But the cost borne by retailers—many of whom are small businesses—is not often acknowledged when discussing identity theft.

---

[4] Brian Grow, Jason Bush, "*Hacker Hunters: An Elite Force Takes on the Dark Side of Computing*", BusinessWeek Online, May 30, 2005
http://www.businessweek.com/magazine/content/05_22/b3935001_mz001.htm

[5] Thomas Lenard and Paul Rubin, "*An Economic Analysis of Notification Requirements for Data Security Breaches"* , The Progress & Freedom Foundation, July 2005 http://www.pff.org/issues-pubs/pops/pop12.12datasecurity.pdf

The remaining third of identity thefts involve someone opening new credit accounts in the victim's name. On average, the person victimized incurs $1,180 in out-of-pocket costs, and spends 60 hours clearing up the mess (although it can take years to clear one's credit record). On average, the businesses that issued or accepted the bogus credit are out by $10,000 each.

Lenard and Rubin report that total costs of $55 billion are borne by both business and consumers, with business incurring $50 billion, or ten times as much as the consumers who are victimized. In no way does this diminish the personal hardships of identity theft that can be devastating to individuals and families –victims can spend hundreds of hours dealing with the damage, and it may take years to clear their name and credit records. But the fact that businesses are hit with ten times as much as consumers explains why business is genuinely committed to reduce the losses due to identity theft.

We've been talking so far only about out-of-pocket costs and time spent by victims, whether business or consumer. The marketplace also imposes substantial costs on businesses that have apparently failed to secure the information entrusted with them. Businesses that lose customer data are punished by the marketplace, as customers leave and competitors pounce on the opportunity posed by a damaged reputation. The Ponemon Institute released a survey of 10,000 adults, drilling into their reactions to security breach notices they've received:

- 20 percent terminated their relationship with the company whose systems were breached.
- An additional 40 percent are considering whether to end the relationship.
- Five percent hired legal counsel after receiving a security breach notification. Up to 50 million Americans who have received notifications, posing a growing risk of lawsuits.

Of course, some breaches occur at businesses that serve other business customers, and don't deal directly with consumers. But large customers are also showing they will terminate relationships with vendors who've been breached, as seen with the CardSystems incident in 2005. It's clear that in choosing where to do business, customers are increasingly asking whether they can trust a business to maintain their data.

THE SMALL BUSINESS PERSPECTIVE

Small business doesn't often come to Congress to request new regulation. But irresistible forces have pushed 35 states[6] to enact their own breach notification laws, leading many businesses to call for a national notification standard. Congress, however, is inclined to combine a national notice requirement with data protection regulation that would extend to small businesses not currently regulated by federal agencies.

The State Stampede to Require Breach Notification

For the past three years, I've worked with businesses of all sizes to educate state lawmakers regarding security breach notification legislation. While not calling for new laws, most businesses acknowledge there are potential benefits to requiring notice of data security breaches:

- The requirement to notify provides an additional incentive for businesses (and state agencies) to tighten-up their information security practices, thus avoiding the embarrassing and expensive consequences of acknowledging a breach. Even businesses in unregulated industries appreciate the risks they face from lawsuits for actual damages occurring as a result of data security breaches.
- Notice requirements can include specific incentives to encourage businesses to use data encryption or other technological means to render data unusable if it's lost or stolen.
- Consumers who receive timely notice can monitor their credit accounts for unauthorized charges, add fraud alerts to their credit reports, and even request that credit reporting agencies stop new accounts from being opened in their name.

However, these potential benefits should be assessed for their likely effect and weighed against costs and unintended consequences:

- Notification by businesses only matters when it's a ***business*** that loses the data. Most identity theft and credit card fraud is done by ***people*** that the victim *actually knows*, so breach notification isn't even a factor.
- Over-notification will occur if consumers receive notices for situations that don't pose a risk of identity theft. And over-notification will de-sensitize consumers to situations of true risk if and when they occur. Most businesses have advocated a risk-based

[6] National Conference of State Legislatures website, at http://www.ncsl.org/programs/lis/CIP/priv/breach.htm

trigger for notice obligations, with incentives to safeguard data through practices such as encrypting or redacting sensitive data, or storing account information in a way that can't be linked with names.

- Businesses should be deemed compliant if they already follow notification requirements imposed by their functional federal regulator. Otherwise, these regulated businesses could be subject to conflicting requirements.
- Notice deadlines need to be realistic, given the time it takes to properly investigate the extent of a breach, verify addresses, and prepare informative and actionable instructions to consumers. Furthermore, regulations should be flexible as to how to communicate most directly and effectively with affected consumers.
- Drafts of some state notification bills created the risk of massive private lawsuits against companies who missed technical notice requirements. In one state, a business that missed a 15-day notice deadline on just 1000 consumers could be sued by plaintiff's attorneys for $1 million, under a provision of existing consumer protection law. State Attorney's General can certainly assess civil fines, and businesses are already susceptible to lawsuits for any actual damages incurred from identity theft or fraud based on data they lost. But there is little justification for empowering the plaintiff's bar to bankrupt a business for a technical failure to notify.

The most significant *unintended* cost of state legislation to require breach notification is that it has created an impossibly complex patchwork of overlapping and often conflicting laws.

An Impossible Patchwork of State Notification Laws

A rush to pass security breach notification bills has already created an unworkable system of inconsistent and incompatible state laws. It's confusing to consumers and makes it nearly impossible for businesses to comply. A small business with customer information from multiple state residents faces the challenge of simultaneously complying with as many as 35 state notification laws.

Consider the coverage of just one state notification law, Pennsylvania's Senate Bill 711, which was signed by Governor Rendell in December, 2005. Pennsylvania's law applies to any "*entity that maintains or manages computerized personal information*." Entity includes a "*state agency, political subdivision, individual or a business doing business in PA"*. While there's no definition for "*doing business"* in this law, if a business has ever invoiced a

customer in Pennsylvania, it is likely to be subject to Pennsylvania's laws in notifying that state's residents of any lost or stolen personal data.

A patchwork of state regulation often prods industry to call upon Congress for a national standard that preempts state laws—something that's unpopular in state capitals. Ironically, however, state security breach laws are *preempting each other*, since most databases include customers from around the country. The only feasible way to comply with different laws is to follow the most restrictive parts of *any* state. For example:

> A business whose breached data included California residents would have to provide notice even when there's no risk of identity theft. Residents of other states with risk-based triggers would be alarmed to hear of the California notices in the media, so the business would have to give the California-style notice to residents of every state. Thus, California can preempt the risk-based trigger mechanism that has been adopted in many states.
>
> If any Illinois customers are among the data that was lost or stolen, Illinois law *doesn't allow a business to delay notification* while cooperating with law enforcement. So the required Illinois notice would compromise investigations being conducted by law enforcement officials in other states.

As you can see, some state laws are effectively preempting other state laws. Perhaps the FTC anticipated this concern with the final instruction of its publication, "Complying with the Safeguards Rule": "*Check to see if breach notification is required under applicable state law*."[7] Any business—large or small—that handles data from customers in many states needs a national standard to mitigate the patchwork of 35 state laws already on the books.

Congress is now weighing several bills that require both notice and data protection regulation, and the small business perspective on two leading bills is discussed below.

Small Business and Data Protection Legislation

Faced with an unworkable patchwork of state laws, a preemptive federal notice law would bring needed relief for business. Unfortunately, Congressional drafts go beyond notification requirements by imposing GLB-style data protection obligations upon small businesses not previously regulated by GLB.

[7] "FTC FACTS for Business, Complying with the Safeguards Rule", Federal Trade Commission, Bureau of Consumer Protection, Office of Consumer and Business Education, April 2006.

Data protection safeguard laws are a significant intrusion into the operations of small businesses, especially those in industries without oversight from a functional regulator. Not every business will need to build a brick house to protect against identity theft wolves, but business will have every incentive to overbuild to reduce regulatory risk.

Several House bills from the 109th and current Congress are related to notification and data protection:

- HR 3140 (109th) "Consumer Data Security and Notification ACT of 2005"
- HR 3997 (109th) "The Financial Data Protection Act of 2006"
- HR 4127 (109th) "The Data Accountability and Trust Act"
- HR 836 (110th) "Cyber-Security Enhancement and Consumer Data Protection Act"
- HR 958 (110th) "Data Accountability and Trust Act"

Four aspects of the small business perspective on these bills are presented next.

1. Many small businesses would be regulated for the first time

Some of these bills significantly expand which businesses are covered by data protection requirements. HR 3140 (109th) would treat previously unregulated small businesses as FINANCIAL INSTITUTIONS, with a definition that includes "*any person or organization that, in the regular course of business, collects and maintains written or electronic files containing individually identifiable information on customer transactions, including any bank, savings association, or credit union account number, credit card or debt card number, and any other payment account number, or any password, access code, or security code pertaining to any such account or any credit card or debit card*."

Similarly, HR 3997 (109th) would encompass anyone "*maintaining, receiving, or communicating sensitive financial personal information on an ongoing basis for the purposes of engaging in interstate commerce*." HR 4127 (109th) would extend safeguards and notification obligations to every person and business "*engaged in interstate commerce that owns or possesses data in electronic form containing personal information*."

These proposed definitions could cover any sales or service business that records its customers' payment methods or stores any quantity of historical payment transactions. *That is, virtually every business that accepts anything other than cash*. Such a significant

expansion of regulation should be carefully constructed to help small businesses work their way into compliance, as described later in this testimony.

2. Requirements for breach notification should be predicated on risk of ID theft or fraudulent transactions

Consumers should be notified when data breaches pose a material risk of ID theft or fraudulent transactions, but Congress should avoid de-sensitizing consumers with over-notification, which has occurred with privacy notices required by GLB. Breaches that don't pose risks to consumers should therefore not drive notification requirements.

Most of the federal breach notice bills considered recently have advocated a risk-based trigger for notice obligations, and provided incentives for safe data practices such as encrypting or redacting sensitive data, or storing account data in a way that can't be linked with customer names.

For example, HR 3140 (109th) would allow businesses to reasonably conclude "that misuse of information is unlikely to occur" if the data were encrypted in accordance with the Advanced Encryption Standard adopted by the National Institute of Standards and Technology for use by the Federal Government.

However, incentives to protect data should anticipate that encryption is not the only mechanism that can effectively protect data, and that new means of protection will be offered in the future. HR 958 (110th) provides for such alternatives to today's encryption "*which renders data in electronic form unreadable or indecipherable, that shall, if applied to such data, establish a presumption that no reasonable risk of identity theft, fraud, or other unlawful conduct exists following a breach of security of such data*." And Senator Carper's bill (S.1260) provides an exception from notice requirements if lost data is maintained in an encrypted, redacted, altered, edited, or coded form that is not usable for purposes of identity theft or to make fraudulent transactions.

Breach notice mandates should include risk-based triggers and encourage the development and use of technologies to render lost or stolen data unusable when it falls into unauthorized hands.

3. State notification laws should be preempted by a national standard

As noted earlier, businesses now acknowledge the need for a national standard to replace a patchwork of 35 state laws governing security breach notification. Legislation considered in the prior and current Congress have offered differing degrees of preemption.

- HR 3997 (109th) contained broad preemption, overriding any state law that regulates the security or confidentiality of consumer information, safeguarding requirements, and investigation or mitigation mandates for data breaches.
- HR 4127 (109th) superseded state regulation of information safeguards and notice for unauthorized data access.
- HR 958 preempts state laws that require security practices or breach notification.

The above bills contain preemption language that would effectively create a uniform national standard for data safeguards and notification. HR 3140, on the other hand, relied upon the preemption level of GLB, which allows states to add more stringent rules if they do not conflict with federal rules. In effect, GLB imposes a floor—but no ceiling—on state regulation, thereby allowing the present state patchwork to persist.

4. Huge penalties could be fatal for small businesses

HR 4127 (109th) created separate penalty schemes for safeguard and notification violations. For safeguard rule violations, civil penalties under HR 4127 were calculated by multiplying the number of violations by a fine of up to $11,000 per. Each day of noncompliance is treated as a separate violation. Penalties for violations of the notification rules are calculated in the same manner, except that each failure to send a notice to an individual is treated as a separate violation.

The multipliers in these notification penalties could mean million dollar fines for a small business who fails to notify only a few hundred consumers. One can imagine the dilemma of a small business owner, upon discovering breaches that his employees should have reported much earlier. In that situation, an owner might avoid a multi-million dollar fine (and bankruptcy) by not reporting the breach, while hoping that it would not lead to any consumer harm. To avoid making this gamble too attractive, Congress should consider alternative ways to limit penalties for a single breach, and perhaps capping breaches that are discovered in a single investigation.

One other breach notification bill holds a nasty surprise for small business. The Cyber-Security Enhancement and Consumer Data protection Act of 2006 (HR 5318 in the 109th) would have made it a criminal offense to fail to report any "major security breach" to law enforcement. For private companies, a "major security breach" is one where "*personal information pertaining to 10,000 or more individuals is, or is reasonably believed to have been acquired*." Owners of small businesses that are not currently regulated would be surprised to learn they face jail terms for failing to report "non-crimes", such as the accidental loss of a portable memory stick or a laptop computer. This bill would require notification of law enforcement when network intrusions are recorded by security monitoring software, without knowledge of whether any personal information was acquired.

GLB-style Safeguards Won't Work for Small Business

While federal legislation would provide relief from the patchwork of state data security laws, this relief could be costly to small businesses if GLB-style data safeguard requirements are imposed on industries not currently regulated by GLB. At least one bill in the 109th Congress (HR 3140) would have imposed GLB data safeguard rules on virtually everyone who maintains any customer account information. In fact, the pain of regulation could exceed the gain of preemption if these data safeguards are unworkable for small business.

At a fundamental level, data safeguard rules may not be justified since businesses already have powerful incentives to protect their customers' data. Legal liability and mandatory notification alone are probably sufficient to discipline businesses that fail to protect customer data.

Adding a data safeguard mandate will undoubtedly add compliance costs and carry unintended consequences, which should be evaluated against the positive effects of this regulation. Other members of this panel are better qualified to assess the effectiveness of the GLB Safeguards in place for the last several years.

Simply put, GLB regulates the handling of consumers' personal financial information, by financial institutions and also by non-traditional financial institutions, such as mortgage brokers and automobile dealers. However, GLB did not cover the vast majority of small businesses that would be regulated if new laws include anyone who handles sensitive financial information for purposes of customer billing and payments.

In 2003, the FTC began enforcing rules to implement the data protection provisions of GLB, known as the "Safeguards Rule".[8] As described in section 314.4 of the CFR (see Appendix B), the required elements of the Safeguards program included a risk assessment, monitoring and control measures. In its rulemaking, the FTC acknowledged concerns for small-entities and sought to "*preserve flexibility and minimize burdens*" on financial institutions subject to the rule.[9]

In the tradeoff between flexible standards and prescriptive requirements, small business will naturally favor flexibility. In technology fields, a one-size-fits-all prescription won't work for everyone on the day it's issued, and won't work for *anyone* as technology moves beyond the originally prescribed solution.

In these federal proposals, it's important to remember that "flexible" doesn't mean "optional". It means that requirements may be adapted to business operations and procedures. A "flexible" regulatory regime acknowledges that solutions may need to be adapted to work-around legacy software and customized in-house systems. However, flexibility in a regulatory standard can also prove confusing and unnecessarily drive up costs for small businesses:

- Small business owners won't be aware of new safeguard requirements if they are in an industry that has not historically been regulated. Many owners will learn for the first time that they are subject to new regulations when they see ads and pitches from software and hardware vendors, system integrators, and consultants –many of whom are ACT members. Each of these marketing messages will describe the problem and solution in different terms, depending upon the vendor's place in the "Security Stack" (Appendix A). Expect confusion and frustration among your small business constituents as they come to realize that they are subject to new regulations.
- Small businesses lack the expertise to select and manage the consultants and vendors needed to design and implement complex data security solutions. For instance, CFR 314(b) calls for a risk assessment, for which most small businesses will have to outsource to an experienced consultant. Most consultants who perform a risk assessment will naturally follow-up with a proposal to mitigate the risks, as a business is required to do under CFR 314(c).

---

[9] *Standards for Safeguarding Customer Information*, 67 Fed Reg 36484 (May 23, 2002).

- Conscientious systems consultants will propose a range of solutions with multiple degrees of data protection. Some proposals will be heavy on up-front costs, while others will spread costs over a long-term service agreement or outsourcing contract. With some costs, the size of small businesses will work to their disadvantage. Data encryption technologies, for example, cost roughly the same for databases with 10,000 records as for 10 million records.

Small Business Needs Flexible Standards plus Best Practices

If flexible standards can be confusing and expensive for small business, what's a better way to help small business implement data protection? ACT believes the answer is to stay with flexible standards, but call upon regulators to take it one step further. Require the FTC to seek, approve, and publish practical and affordable "best practices" that meet the flexible standard.

The FTC should look to industry for candidate best practices, since industry has the skills and incentives to implement approved solutions for regulated businesses. For example, leaders in the credit card industry responded to GLB Safeguard rules by developing a consensus approach for merchants who accept their cards for payment. Their Payment Card Industry Data Security Standard ("PCI Standard") is now part of the contract for any business that wants to accept credit card payments.[10]

Unfortunately, the PCI Standard is not simple enough to be a model for all small businesses. The current version is 12 pages long and sets forth 176 individual requirements grouped into a dozen major requirements. To be usable by previously-unregulated businesses, each requirement will need to be fleshed-out with specific examples of compliant behavior and/or specific product solutions.

Regulators should also be required to evaluate potential solutions for data protection compliance, and to publish an online catalog of results.

What we don't want to see is another "*Small-Entity Compliance Guide*" for Interagency Guidelines[11]. Though undertaken with the best intentions, this guide is of little

[10] www.visa.com/cisp

[11] "Interagency Guidelines Establishing Information Security Standards, Small-Entity Compliance Guide", at http://www.federalreserve.gov/Regulations/cg/infosec.htm

help to small business. It just reiterates FTC Safeguard Rules, without providing specific guidance on solutions for small business.[12].

These *Interagency Guidelines* are not likely to help small business owners to select and implement practical and affordable data protection solutions. There is much work to be done by regulators and by industry to reach that goal, which becomes essential if regulations such as the GLB Safeguards are applied to every small business who handles sensitive financial information for billing customers and booking payments.

Conclusion

We are grateful to this subcommittee for its continued vigilance on behalf of small business owners. As you consider data protection regulation, we ask that you act as our "angel" with House leadership and in conference committee.

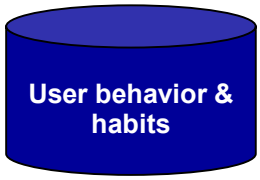
Please use your significant influence to drive regulators to help small business understand and meet data protection standards without spending far more than they need to. Data protection standards should be flexible, yet regulators should quickly seek, evaluate, and approve multiple best practices that meet the standard.

Moreover, until regulators have published approved best practices suitable and affordable for small business compliance, please consider a temporary exemption from new data protection requirements for small entities—especially those businesses who were not previously covered by a federal functional regulator.

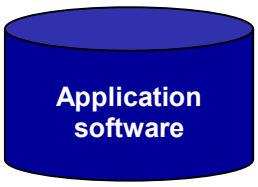
[12] Section 314.3 (b)(1), "*Standards for Safeguarding Customer Information"*, 67 Fed Reg 36494, May 23, 2002. The Small-Entity Guide warns that "*Insurance coverage is not a substitute for an information security program.*"[12] Perhaps it was necessary to clarify that the FTC meant "*ensure*" when it actually wrote, "*Insure* the security and confidentiality of customer information

APPENDIX A: The Security Stack

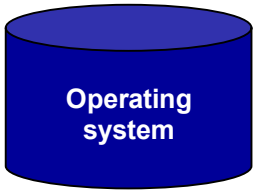
Responses to security threats happen at multiple layers of a "security stack" that starts with user behavior, includes hardware and software solutions, and rests on a foundation of network security.



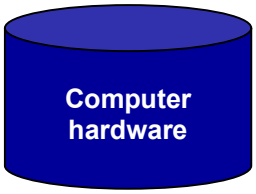
User behavior and habits are security practices, ranging from the everyday behavior of employees to the top of IT management. This layer includes the acquisition, installation, maintenance, and application of updates. Users are fundamental to the security stack, since most attacks are facilitated by some aspect of user behavior. For example, 86% of respondents in a 2002 FBI survey reported an information security attack in the form of an e-mail attachment.



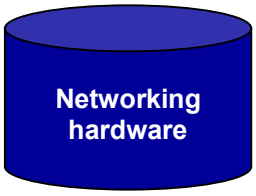
Application software includes productivity tools such as e-mail, word processors, spreadsheets, databases, instant messaging, browsers, firewalls, and anti-virus software. In the late 1990's, the application layer was often attacked with viruses propagating through vulnerabilities in e-mail clients or through macros embedded in documents.



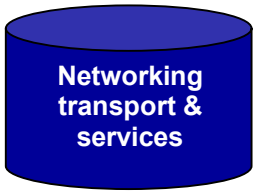
Operating systems are the central layer of the security stack, both on client and server computers. On the client-side desktop environment, the Operating system layer includes Windows, Linux, and Apple. Server-side products include Microsoft Server, Sun Solaris, Novell, UNIX, and enterprise Linux. The server space has become the preferred target for malware makers seeking increased speed and scope of propagation.



Computer hardware includes desktop PCs, laptops, cell phones, PDAs, and pocket PCs. Although generally not the main target today, makers of these hardware devices are becoming more security-conscious. Industry efforts include processors with strong process isolation and sealed data storage devices.



Networking hardware includes routers and switches that serve as network gateways and firewalls that monitor incoming and outgoing traffic. This layer also includes an emerging device layer of appliances, offered by McAfee and other vendors that work to block spam and other suspect traffic to further augment security at the perimeter.



Networking transport & services is the layer outside our business walls. This layer includes packet monitoring and filtering by ISPs and Web infrastructure providers, who monitor Internet traffic, identify anomalies in the volume or nature of traffic, and act accordingly by notifying or blocking affected hosts and users.

APPENDIX B: FTC Safeguard Standards

16 CFR PART 314—STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

Authority: 15 U.S.C. 6801(b), 6805(b)(2).

§ 314.1 Purpose and scope.

(a) *Purpose.* This part, which implements sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act, sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

(b) *Scope.* This part applies to the handling of customer information by all financial institutions over which the Federal Trade Commission (''FTC'' or ''Commission'') has jurisdiction. This part refers to such entities as ''you.''

This part applies to all customer information in your possession, regardless of whether such information pertains to individuals with whom you have a customer relationship, or pertains to the customers of other financial institutions that have provided such information to you.

§ 314.2 Definitions.

(a) *In general.* Except as modified by this part or unless the context otherwise requires, the terms used in this part have the same meaning as set forth in the Commission's rule governing the Privacy of Consumer Financial Information, 16 CFR part 313.

(b) *Customer information* means any record containing nonpublic personal information as defined in 16 CFR 313.3(n), about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.

(c) *Information security program* means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

(d) *Service provider* means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to this part.

§ 314.3 Standards for safeguarding customer information.

(a) *Information security program.* You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. Such safeguards shall include the elements set forth in § 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

(b) *Objectives.* The objectives of section 501(b) of the Act, and of this part, are to:

(1) Insure the security and confidentiality of customer information;

(2) Protect against any anticipated threats or hazards to the security or integrity of such information; and

(3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

§ 314.4 Elements.

In order to develop, implement, and maintain your information security program, you shall:

(a) Designate an employee or employees to coordinate your information security program.

(b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a

minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

(1) Employee training and management;

(2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

(d) Oversee service providers, by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

(2) Requiring your service providers by contract to implement and maintain such safeguards.

(e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

From http://www.access.gpo.gov/nara/cfr/waisidx_03/16cfr314_03.html